

UREDBA (EU) 2018/1807 EVROPSKEGA PARLAMENTA IN SVETA**z dne 14. novembra 2018****o okviru za prosti pretok neosebni podatkov v Evropski uniji****(Besedilo velja za EGP)**

EVROPSKI PARLAMENT IN SVET EVROPSKE UNIJE STA –

ob upoštevanju Pogodbe o delovanju Evropske unije in zlasti člena 114 Pogodbe,

ob upoštevanju predloga Evropske komisije,

po posredovanju osnutka zakonodajnega akta nacionalnim parlamentom,

ob upoštevanju mnenja Evropskega ekonomsko-socialnega odbora ⁽¹⁾,

po posvetovanju z Odborom regij,

v skladu z rednim zakonodajnim postopkom ⁽²⁾,

ob upoštevanju naslednjega:

- (1) Digitalizacija gospodarstva poteka vedno hitreje. Informacijske in komunikacijske tehnologije niso več poseben sektor, temveč temelj vseh modernih inovativnih gospodarskih sistemov in družb. V središču navedenih sistemov so elektronski podatki, s katerimi se lahko ustvari visoka vrednost, kadar se analizirajo ali združujejo s storitvami in izdelki. Obenem se zaradi hitrega razvoja podatkovnega gospodarstva in tehnologij v vzponu, kot so umetna inteligenca, proizvodi in storitve interneta stvari, avtonomni sistemi ter 5G, porajajo nova pravna vprašanja, povezana z dostopom do podatkov in njihovo ponovno uporabo, odgovornostjo, etiko in solidarnostjo. Treba bi bilo premisliti o delu v zvezi z vprašanjem odgovornosti, zlasti prek izvajanja samoregulativnih kodeksov ravnanja in druge najboljše prakse, ob upoštevanju priporočil, sklepov in ukrepov, sprejetih brez človekovega posredovanja vzdolž celotne vrednostne verige obdelave podatkov. To delo bi lahko tudi vključevalo ustrezne mehanizme za ugotavljanje odgovornosti, za prenos odgovornosti med sodelujočimi službami ter za zavarovanje in revizijo.
- (2) Podatkovne vrednostne verige vključujejo različne dejavnosti v zvezi s podatki: ustvarjanje in zbiranje podatkov; združevanje in organizacija podatkov; obdelava podatkov; analiza, trženje in razširjanje podatkov; uporaba in ponovna uporaba podatkov. Uspešno in učinkovito delovanje obdelave podatkov je temeljni gradnik vsake podatkovne vrednostne verige. Vendar uspešno in učinkovito delovanje obdelave podatkov ter razvoj podatkovnega gospodarstva v Uniji omejujeta zlasti dve vrsti ovir v zvezi z mobilnostjo podatkov in v zvezi z notranjim trgov: zahteve glede lokalizacije podatkov, ki jih uvedejo organi držav članic, in prakse, ki pripeljejo do vezanosti na ponudnika v zasebnem sektorju.
- (3) Svoboda ustanavljanja in svoboda opravljanja storitev iz Pogodbe o delovanju Evropske unije (PDEU) se uporabljata za storitve obdelave podatkov. Vendar opravljanje navedenih storitev ovirajo ali včasih preprečujejo določene nacionalne, regionalne ali lokalne zahteve za lokalizacijo podatkov na določenem ozemlju.
- (4) Takšne ovire za prosti pretok storitev obdelave podatkov ali ovire pravice do ustanavljanja ponudnikov storitev izhajajo iz zahtev v pravu držav članic, da se za namen obdelave podatkov, podatki lokalizirajo na določenem geografskem območju ali ozemlju. Enakovreden učinek imajo tudi druga pravila ali upravne prakse, ki vsebujejo posebne zahteve, ki otežujejo obdelavo podatkov zunaj določenega geografskega območja ali ozemlja v Uniji, kot so zahteve za uporabo tehnoloških naprav, certificiranih ali odobrenih v določeni državi članici. Možnosti izbire, ki so v zvezi z lokacijo obdelave podatkov na voljo subjektom na trgu in javnemu sektorju, nadalje omejuje pravna negotovost pri obsegu zakonitih in nezakonitih zahtev glede lokalizacije podatkov. Ta uredba z ničemer ne omejuje svobode podjetij, da sklepajo pogodbe, ki določajo lokacijo podatkov. Namen te uredbe je zgolj ohraniti to svobodo z zagotovitvijo, da se lahko dogovorjena lokacija nahaja kjerkoli v Uniji.

⁽¹⁾ UL C 227, 28.6.2018, str. 78.⁽²⁾ Stališče Evropskega parlamenta z dne 4. oktobra 2018 (še ni objavljeno v Uradnem listu) in odločitev Sveta z dne 6. novembra 2018.

- (5) Mobilnost podatkov v Uniji hkrati ovirajo tudi zasebne omejitve: pravna, pogodbeni in tehnični vprašanja, ki uporabnike storitev obdelave podatkov ovirajo pri prenosu svojih podatkov od enega ponudnika storitev do drugega ali nazaj v lastne sisteme informacijske tehnologije ali jim ta prenos preprečujejo, zlasti ob prenehanju pogodbe s ponudnikom storitev.
- (6) Kombinacija teh ovir je vodila do odsotnosti konkurence med ponudniki storitev v oblaku v Uniji, do različnih vprašanj glede vezanosti na ponudnika, in do zelo pomanjkljive mobilnosti podatkov. Prav tako so politike lokalizacije podatkov podjetjem za raziskave in razvoj otežile zagotavljanje sodelovanja med podjetji, univerzami in drugimi raziskovalnimi organizacijami, da bi se spodbujale inovacije.
- (7) Zaradi pravne varnosti in zaradi potrebe po enakih konkurenčnih pogojih v Uniji je enoten sklop pravil za vse udeležence na trgu ključnega pomena za delovanje notranjega trga. Za odpravo ovir pri trgovini in izkrivljanju konkurence, ki so posledica razlik med nacionalnimi zakonodajami, ter za preprečitev nastanka morebitnih dodatnih ovir pri trgovini in znatnih izkrivljanju konkurence je treba sprejeti enotna pravila, ki se bodo uporabljala v vseh državah članicah.
- (8) Ta uredba ne vpliva na pravni okvir o varstvu fizičnih oseb glede obdelave osebnih podatkov, na spoštovanje zasebnega življenja in na varstvo osebnih podatkov v elektronskih komunikacijah, ter zlasti na Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta ⁽¹⁾ in direktivi (EU) 2016/680 ⁽²⁾ in 2002/58/ES ⁽³⁾ Evropskega parlamenta in Sveta.
- (9) Čedalje bolj razširjeni internet stvari, umetna inteligenca in strojno učenje predstavljajo glavne vire neosebnih podatkov, ko se npr. uporabljajo v postopkih avtomatizirane industrijske proizvodnje. Specifični primeri neosebnih podatkov vključujejo združene in anonimizirane podatkovne nize, ki se uporabljajo pri analizi masovnih podatkov, podatke o preciznem kmetovanju, ki lahko pomagajo pri spremljanju in optimizaciji uporabe pesticidov in vode, ali podatke o potrebah po vzdrževanju industrijskih strojev. Če bo tehnološki napredek omogočil pretvorbo anonimiziranih podatkov v osebne, bi se morali takšni podatki obravnavati kot osebni podatki, ob ustrezni uporabi Uredbe (EU) 2016/679.
- (10) V skladu z Uredbo (EU) 2016/679 države članice ne smejo niti omejiti niti prepovedati prostega pretoka osebnih podatkov v Uniji iz razlogov, povezanih z varstvom posameznikov pri obdelavi osebnih podatkov. Ta uredba določa enako načelo prostega pretoka v Uniji za neosebne podatke, razen ko je omejitev ali prepoved upravičena iz razlogov javne varnosti. Uredba (EU) 2016/679 in ta uredba določata enoten sklop pravil, ki urejajo prosti pretok različnih vrst podatkov. Poleg tega ta uredba ne nalaga obveznosti ločenega shranjevanja različnih vrst podatkov.
- (11) Za vzpostavitev okvira za prosti pretok neosebnih podatkov v Uniji ter temeljev za razvoj podatkovnega gospodarstva in boljše konkurenčnost industrije Unije je treba določiti jasen, celovit in predvidljiv pravni okvir za obdelavo podatkov, ki niso osebni podatki, na notranjem trgu. S pristopom, ki temelji na načelih sodelovanja med državami članicami, in samoregulacijo bi se morala zagotoviti takšna prožnost okvira, da bi se lahko upoštevale spreminjajoče se potrebe uporabnikov, ponudnikov storitev in nacionalnih organov v Uniji. Da bi se izognili tveganju prekrivanja z obstoječimi mehanizmi, in s tem večjim bremenom za države članice in podjetja, ne bi smela biti določena podrobna tehnična pravila.
- (12) Ta uredba ne bi smela vplivati na obdelavo podatkov, v kolikor se izvaja kot del dejavnosti, ki ne spada na področje uporabe prava Unije. Zlasti bi bilo treba opozoriti, da v skladu s členom 4 Pogodbe o Evropski uniji (PEU) nacionalna varnost ostaja v izključni pristojnosti vsake države članice.

⁽¹⁾ Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1).

⁽²⁾ Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ (UL L 119, 4.5.2016, str. 89).

⁽³⁾ Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31.7.2002, str. 37).

- (13) Prosti pretok podatkov v Uniji bo imel pomembno vlogo pri doseganju rasti in inovacij, ki temeljijo na podatkih. Tako kot podjetja in potrošniki imajo tudi javni organi in osebe javnega prava držav članic koristi od večje svobode izbire, kar zadeva ponudnike podatkovnih storitev, od konkurenčnejših cen in od učinkovitejšega zagotavljanja storitev državljanom. Glede na velike količine podatkov, ki jih obdelujejo javni organi in osebe javnega prava, je ključnega pomena, da dajejo zgled z uporabo storitev obdelave podatkov in ne določajo omejitev za lokalizacijo podatkov, kadar uporabljajo storitev obdelave podatkov. Zato bi morala ta uredba zajemati tudi javne organe in osebe javnega prava. V zvezi s tem bi se moralo načelo prostega pretoka neosebnih podatkov iz te uredbe uporabljati tudi za splošne in dosledne administrativne prakse in za druge zahteve glede lokalizacije podatkov na področju javnega naročanja, brez poseganja v Direktivo 2014/24/EU Evropskega parlamenta in Sveta ⁽¹⁾.
- (14) Kot v primeru Direktive 2014/24/EU, ta uredba ne posega v zakone in druge predpise v zvezi z notranjo organizacijo držav članic, ki določajo prenos pristojnosti in pooblastil za obdelavo podatkov brez pogodbenih plačil zasebnih strank na javne organe in osebe javnega prava, kot tudi ne v zakone in druge predpise držav članic, ki določajo izvajanje teh pooblastil in pristojnosti. Medtem ko se javne organe in osebe javnega prava spodbuja, naj preučijo gospodarske in druge prednosti oddajanja v zunanje izvajanje zunanjim ponudnikom storitev, bi ti lahko imeli legitimne razloge za izbiro samozagotavljanja storitev ali notranjega izvajanja. Zato nič v tej uredbi ne obvezuje držav članic, da sklepajo pogodbe z zunanjimi izvajalci ali da nanje prenesejo opravljanje storitev, ki jih želijo opravljati sami ali jih organizirati na drug način kot pa z javnimi naročili.
- (15) Ta uredba bi se morala uporabljati za fizične ali pravne osebe, ki ponujajo storitve obdelave podatkov uporabnikom, ki prebivajo ali imajo sedež v Uniji, vključno s tistimi, ki ponujajo storitve obdelave podatkov v Uniji in nimajo sedeža v Uniji. Ta uredba se zato ne bi smela uporabljati za storitve obdelave podatkov, ki potekajo zunaj Unije, in za zahteve glede lokalizacije podatkov, ki zadevajo te podatke.
- (16) Ta uredba ne določa pravil v zvezi z določitvijo prava, ki se uporablja v gospodarskih zadevah, in zato ne posega v Uredbo (ES) št. 593/2008 Evropskega parlamenta in Sveta ⁽²⁾. Zlasti za pogodbo o opravljanju storitev načeloma velja pravo države, v kateri ima ponudnik storitev običajno prebivališče, če pravo, ki se uporablja za pogodbo, ni bilo izbrano v skladu z navedeno uredbo.
- (17) Ta uredba bi se morala uporabljati za obdelavo podatkov v najširšem smislu ter vključevati uporabo vseh vrst informacijskih sistemov, ne glede na to, ali se nahajajo v prostorih uporabnika ali se oddajo v zunanje izvajanje ponudniku storitev. Zajemati bi morala obdelavo podatkov na različnih ravneh intenzivnosti, od shranjevanja podatkov (infrastruktura kot storitev (IaaS)) do obdelave podatkov na platformah (platforma kot storitev (PaaS)) ali v aplikacijah (programska oprema kot storitev (SaaS)).
- (18) Zahteve glede lokalizacije podatkov nedvomno ovirajo prosto opravljanje storitev obdelave podatkov v Uniji in predstavljajo ovire delovanja notranjega trga. Zato bi jih bilo kot take treba prepovedati, razen če so utemeljene iz razlogov javne varnosti, kot je opredeljeno s pravom Unije, zlasti v smislu člena 52 PDEU, in upoštevajo načelo sorazmernosti iz člena 5 PEU. Da bi se uveljavilo načelo prostega pretoka neosebnih podatkov prek meja, zagotovila hitra odprava obstoječih zahtev glede lokalizacije podatkov ter da bi se iz operativnih razlogov omogočila obdelava podatkov na več lokacijah v Uniji in ker ta uredba določa ukrepe za zagotovitev razpoložljivosti podatkov za namene regulativnega nadzora, bi se države članice lahko sklicevale na javno varnost le kot utemeljitev zahteve glede lokalizacije podatkov.
- (19) Pojem „javne varnosti“ v smislu člena 52 PDEU in kot ga razlaga Sodišče, zajema tako notranjo kot zunanjo varnost države članice ter vprašanja varnosti ljudi, zlasti za olajšanje preiskovanja, odkrivanja in pregona kaznivih dejanj. Predpostavlja obstoj dejanske in dovolj resne grožnje, ki vpliva na enega od temeljnih interesov družbe, kot je ogrožanje delovanja institucij in temeljnih javnih služb ter preživetja prebivalstva, pa tudi tveganje resnih motenj v zunanjih odnosih ali v mirnem sobivanju narodov oziroma grožnjo vojaškim interesom. V skladu z načelom sorazmernosti bi morale biti zahteve glede lokalizacije podatkov, ki so utemeljene z razlogi javne varnosti, primerne za uresničitev zastavljenega cilja in ne bi smele presežati tistega, kar je potrebno za doseganje tega cilja.

⁽¹⁾ Direktiva 2014/24/EU Evropskega parlamenta in Sveta z dne 26. februarja 2014 o javnem naročanju in razveljavitvi Direktive 2004/18/ES (UL L 94, 28.3.2014, str. 65).

⁽²⁾ Uredba (ES) št. 593/2008 Evropskega parlamenta in Sveta z dne 17. junija 2008 o pravu, ki se uporablja za pogodbeno obligacijska razmerja (Rim I) (UL L 177, 4.7.2008, str. 6).

- (20) Da bi se zagotovila učinkovita uporaba načela prostega pretoka neosebnih podatkov prek meja in preprečilo nastajanje novih ovir za nemoteno delovanje notranjega trga, bi morale države članice Komisijo nemudoma obvestiti o vsakem osnutku akta, ki uvaja novo zahtevo glede lokalizacije podatkov ali spreminja obstoječo zahtevo glede lokalizacije podatkov. Te osnutke aktov bi bilo treba predložiti in oceniti v skladu z Direktivo (EU) 2015/1535 Evropskega parlamenta in Sveta ⁽¹⁾.
- (21) Nadalje, da bi se odpravile morebitne obstoječe ovire, bi morale države članice v prehodnem obdobju 24 mesecev po dnevu začetka uporabe te uredbe pregledati obstoječe zakone in druge splošne predpise, ki določajo zahteve glede lokalizacije podatkov, ter Komisiji sporočiti vse tovrstne zahteve glede lokalizacije podatkov, za katere menijo, da so v skladu s to uredbo, skupaj z njihovo utemeljitvijo. To bi moralo Komisiji omogočiti, da pregleda skladnost preostalih zahtev glede lokalizacije podatkov. Komisija bi morala imeti možnost, da, kjer je to primerno, zadevni državi članici poda pripombe. Te pripombe bi lahko vključevale tudi priporočilo za spremembo ali razveljavitev zahteve glede lokalizacije podatkov.
- (22) Obveznosti za sporočanje obstoječih zahtev glede lokalizacije podatkov in osnutkov aktov Komisiji, določene s to uredbo, bi se morale uporabljati za regulativne zahteve glede lokalizacije podatkov in osnutke splošnih pravnih aktov, ne pa za odločitve, ki naslavljajo konkretno fizično ali pravno osebo.
- (23) Da bi se v državah članicah zagotovila preglednost zahtev glede lokalizacije podatkov, določenih v zakonih in drugih splošnih predpisih, za fizične in pravne osebe, kot so ponudniki storitev in uporabniki storitev obdelave podatkov, bi morale države članice informacije o takšnih zahtevah objavljati na nacionalni enotni spletni informacijski točki in te informacije redno posodabljati. Alternativno bi morale države članice o takšnih ukrepih zagotoviti posodobljene informacije centralni informacijski točki, ki jo vzpostavlja drug akt Unije. Za ustrezno obveščanje fizičnih in pravnih oseb o zahtevah glede lokalizacije podatkov v Uniji bi morale države članice Komisijo uradno obvestiti o naslovih teh enotnih informacijskih točk. Komisija bi morala te informacije objaviti na svojem spletišču skupaj z redno posodobljenim zbirnim seznamom vseh zahtev glede lokalizacije podatkov, ki veljajo v državah članicah, vključno s povzetki informacij o omenjenih zahtevah.
- (24) Zahteve glede lokalizacije podatkov pogosto izvirajo iz pomanjkanja zaupanja v čezmejno obdelavo podatkov, saj se predpostavlja, da podatki niso razpoložljivi za namene pristojnih organov držav članic, kot so inšpekcijski pregledi in revizije za regulativne ali nadzorne namene. Takega pomanjkanja zaupanja ni mogoče odpraviti samo prek ničnosti pogodbenih pogojev, ki prepovedujejo zakonit dostop pristojnih organov do podatkov z namenom opravljanja njihovih uradnih dolžnosti. Zato bi morala ta uredba jasno določiti, da ne posega v pooblastila pristojnih organov, da v skladu s pravom Unije ali nacionalnim pravom zahtevajo ali pridobijo dostop do podatkov, in da se pristojnim organom dostop do podatkov ne sme zavrnil na podlagi dejstva, da se podatki obdelujejo v drugi državi članici. Pristojni organi bi lahko uvedli funkcionalne zahteve v podporo dostopu do podatkov, kot je zahteva, da morajo biti opisi sistemov shranjeni v zadevni državi članici.
- (25) Fizične ali pravne osebe, za katere veljajo obveznosti zagotavljanja podatkov pristojnim organom, lahko takšne obveznosti izpolnijo z zagotavljanjem in jamčenjem učinkovitega in pravočasnega elektronskega dostopa do podatkov pristojnim organom, ne glede na državo članico, na ozemlju katere so podatki obdelani. Takšen dostop se lahko zagotovi s konkretnimi pogoji v pogodbah med fizično ali pravno osebo, za katero velja obveznost zagotavljanja dostopa, in ponudnikom storitev.
- (26) Kadar fizična ali pravna oseba, za katero veljajo obveznosti zagotavljanja podatkov, te obveznosti ne izpolni, bi moral imeti pristojni organ možnost, da zaprosi za pomoč pristojne organe v drugih državah članicah. V takšnih primerih bi morali pristojni organi uporabiti posebne sodelovalne instrumente iz prava Unije ali na podlagi mednarodnih sporazumov glede na predmet urejanja v posameznem primeru, kot na primer za področje

⁽¹⁾ Direktiva (EU) 2015/1535 Evropskega parlamenta in Sveta z dne 9. septembra 2015 o določitvi postopka za zbiranje informacij na področju tehničnih predpisov in pravil za storitve informacijske družbe (UL L 241, 17.9.2015, str. 1).

policijskega sodelovanja, pravosodnega sodelovanja v civilnih in kazenskih zadevah oziroma sodelovanja v upravnih zadevah, v Okvirnem sklepu Sveta 2006/960/PNZ⁽¹⁾, Direktivi Evropskega parlamenta in Sveta 2014/41/EU⁽²⁾, Konvenciji Sveta Evrope o kibernetiki kriminaliteti⁽³⁾, Uredbi Sveta (ES) št. 1206/2001⁽⁴⁾, Direktivi Sveta 2006/112/ES⁽⁵⁾ in Uredbi Sveta (EU) št. 904/2010⁽⁶⁾. Kadar takšnih sodelovalnih mehanizmov ni, bi morali pristojni organi sodelovati med seboj, da bi se zagotovil dostop do zaprošenih podatkov prek imenovanih enotnih kontaktnih točk.

- (27) Kadar prošnja za pomoč vključuje, da zaproseni organ pridobi dostop do prostorov fizične ali pravne osebe, vključno z vso opremo in sredstvi za obdelavo podatkov, mora biti takšen dostop v skladu s pravom Unije ali nacionalnim postopkovnim pravom, vključno z morebitno zahtevo po pridobitvi predhodne sodne odobritve.
- (28) Ta uredba uporabnikom ne bi smela omogočati možnosti za izogibanje uporabi nacionalnega prava. Zato bi morala določiti, da države članice naložijo učinkovite, sorazmerne in odvračilne kazni za uporabnike, ki pristojnim organom preprečujejo dostop do svojih podatkov, potrebnih za opravljanje uradnih dolžnosti pristojnih organov na podlagi prava Unije in nacionalnega prava. V nujnih primerih, ko uporabnik zlorabi svoje pravice, bi morale imeti države članice možnost, da določijo strogo sorazmerne začasne ukrepe. Vsi začasni ukrepi, ki predpisujejo relokalizacijo podatkov za obdobje, daljše od 180 dni po relokalizaciji, bi odstopali od načela prostega pretoka podatkov za daljše časovno obdobje in bi jih bilo zato treba sporočiti Komisiji, da preveri njihovo skladnost s pravom Unije.
- (29) Možnost neoviranega prenosa podatkov je ključni dejavnik pri olajševanju izbire uporabnikom ter omogoča učinkovito konkurenco na trgih storitev obdelave podatkov. Prav tako dejanske ali domnevne težave pri čezmejnem prenosu podatkov spodbujajo zaupanje poklicnih uporabnikov v čezmejne ponudbe in s tem v notranji trg. Medtem ko potrošnikom posameznikom obstoječe pravo Unije koristi, pa uporabnikom, ki izvajajo poslovne ali poklicne dejavnosti, ni olajšana možnost zamenjave ponudnika storitev. Dosledne tehnične zahteve po vsej Uniji, bodisi v zvezi s tehnično harmonizacijo, vzajemnim priznavanjem ali prostovoljno harmonizacijo, prav tako prispevajo k razvoju konkurenčnega notranjega trga za storitve obdelave podatkov.
- (30) Da bi v celoti izkoristili konkurenčno okolje, bi morali imeti poklicni uporabniki možnost ozaveščenega odločanja in preproste primerjave posameznih komponent različnih storitev obdelave podatkov, ki jih ponuja notranji trg, vključno v zvezi s pogodbenimi pogoji za prenos podatkov ob prenehanju pogodbe. Za uskladitev z inovacijskim potencialom trga ter upoštevanje izkušenj in strokovnega znanja ponudnikov storitev in poklicnih uporabnikov storitev obdelave podatkov, bi morali podrobne informacije in operativne zahteve za prenos podatkov s samoregulacijo opredeliti subjekti na trgu v obliki kodeksov ravnanja na ravni Unije, ki lahko vključujejo vzorčne pogodbene pogoje, kar bi spodbujala, olajševala in spremljala Komisija.
- (31) Da bi bili navedeni kodeksi ravnanja učinkoviti ter da bi omogočili lažjo zamenjavo ponudnikov storitev in lažji prenos podatkov, bi morali biti razumljivi in bi morali zajemati vsaj ključne vidike, ki so pomembni med procesom prenosa podatkov, ko so procesi za varnostne kopije podatkov in njihove lokacije, razpoložljivi formati in nosilci podatkov, zahtevana konfiguracija informacijske tehnologije ter najmanjša pasovno širino omrežja, čas, ki je potreben pred začetkom postopka prenosa, in čas, v katerem bodo podatki ostali na voljo za prenos podatkov, ter jamstva za dostop do podatkov v primeru stečaja ponudnika storitev. Kodeksi ravnanja bi morali tudi pojasniti, da vezanost na ponudnika ni sprejemljiva poslovna praksa, omogočati bi morali tehnologije, ki povečujejo zaupanje, obenem pa bi jih bilo treba redno posodabljeni, da bodo sledili tehnološkemu razvoju. Komisija bi morala zagotoviti, da bo v proces vključeno posvetovanje z vsemi ustreznimi deležniki, vključno z združenji malih in srednjih podjetij ter zagonskih podjetij, uporabniki in ponudniki storitev v oblaku. Komisija bi morala oceniti razvoj in učinkovitost izvajanja takšnih kodeksov ravnanja.

⁽¹⁾ Okvirni sklep Sveta 2006/960/PNZ z dne 18. decembra 2006 o poenostavitvi izmenjave informacij in obveščevalnih podatkov med organi kazenskega pregona držav članic Evropske unije (UL L 386, 29.12.2006, str. 89).

⁽²⁾ Direktiva Evropskega parlamenta in Sveta 2014/41/EU z dne 3. aprila 2014 o evropskem preiskovalnem nalogu v kazenskih zadevah (UL L 130, 1.5.2014, str. 1).

⁽³⁾ Konvencija Sveta Evrope o kibernetiki kriminaliteti, CETS št. 185.

⁽⁴⁾ Uredba Sveta (ES) št. 1206/2001 z dne 28. maja 2001 o sodelovanju med sodišči držav članic pri pridobivanju dokazov in civilnih ali gospodarskih zadevah (UL L 174, 27.6.2001, str. 1).

⁽⁵⁾ Direktiva Sveta 2006/112/ES z dne 28. novembra 2006 o skupnem sistemu davka na dodano vrednost (UL L 347, 11.12.2006, str. 1).

⁽⁶⁾ Uredba Sveta (EU) št. 904/2010 z dne 7. oktobra 2010 o upravnem sodelovanju in boju proti goljufijam na področju davka na dodano vrednost (UL L 268, 12.10.2010, str. 1).

- (32) Kadar bi pristojni organ v eni državi članici zaprosil drugo državo članico za pomoč pri pridobitvi dostopa do podatkov v skladu s to uredbo, bi moral prek imenovane enotne kontaktne točke na enotno kontaktno točko, ki jo imenuje zaprosena država članica, nasloviti ustrezno utemeljeno prošnjo, v katero bi moral vključiti pisno pojasnitev razlogov in pravno podlago za pridobitev dostopa do podatkov. Enotna kontaktna točka, ki jo imenuje zaprosena država članica, bi morala olajšati posredovanje prošnje ustreznemu pristojnemu organu v zaproseni državi članici. Za zagotovitev učinkovitega sodelovanja bi moral organ, ki mu je posredovana prošnja, brez nepotrebnega odlašanja ugoditi zadevni prošnji in zagotoviti pomoč ali sporočiti, zakaj ima težave pri ugoditvi prošnji za pomoč, ali navesti razloge za njeno zavrnitev.
- (33) S spodbujanjem zaupanja v varnost čezmejne obdelave podatkov bi se morala zmanjšati nagnjenost subjektov na trgu in javnega sektorja k uporabi lokalizacije podatkov kot nadomestka za varnost podatkov. Prav tako bi se morala za podjetja izboljšati pravna varnost v zvezi z izpolnjevanjem veljavnih varnostnih zahtev, kadar dejavnosti obdelave podatkov oddajo v zunanje izvajanje ponudnikom storitev, tudi tistim v drugih državah članicah.
- (34) Vse varnostne zahteve v zvezi z obdelavo podatkov, ki se uporabljajo utemeljeno in sorazmerno na podlagi prava Unije ali nacionalnega prava v skladu pravom Unije, v državi članici, v kateri prebivajo ali imajo sedež fizične ali pravne osebe, ki jim pripadajo zadevni podatki, bi se morale še naprej uporabljati za obdelavo teh podatkov tudi v drugi državi članici. Te fizične ali pravne osebe bi morale imeti možnost izpolniti takšne zahteve bodisi same bodisi prek pogodbenih klavzul v pogodbah s ponudniki storitev.
- (35) Varnostne zahteve, določene na nacionalni ravni, bi morale biti obvezne in sorazmerne s tveganji za varnost obdelave podatkov v okviru nacionalnega prava, ki določa te zahteve.
- (36) Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta ⁽¹⁾ določa pravne ukrepe za povečanje splošne ravni kibernetске varnosti v Uniji. Storitve obdelave podatkov spadajo v eno izmed digitalnih storitev, ki jih zajema navedena direktiva. V skladu z navedeno direktivo morajo države članice zagotoviti, da ponudniki digitalnih storitev določijo in sprejmejo ustrezne in sorazmerne tehnične in organizacijske ukrepe za obvladovanje tveganj za varnost omrežij in informacijskih sistemov, ki jih uporabljajo. S takšnimi ukrepi bi se morala zagotoviti raven varnosti, ki je primerna glede na tveganje, pri čemer bi se morali upoštevati varnost sistemov in zmogljivosti, obvladovanje incidentov, upravljanje neprekinjenega poslovanja, spremljanje, revidiranje in preizkušanje ter skladnost z mednarodnimi standardi. Te elemente naj bi Komisija natančneje določila z izvedbenimi akti v skladu z navedeno direktivo.
- (37) Komisija bi morala predložiti poročilo o izvajanju te uredbe, zlasti zaradi ugotavljanja, ali so glede na tehnološki ali tržni razvoj potrebne spremembe. V tem poročilu bi bilo treba zlasti oceniti to uredbo, predvsem njeno uporabo pri podatkovnih nizih, ki so sestavljeni iz osebnih in neosebnih podatkov, ter izvajanje izjeme glede javne varnosti. Komisija bi morala pred začetkom uporabe te uredbe objaviti tudi informativne smernice o tem, kako ravnati s podatkovnimi nizi, ki so sestavljeni iz osebnih in neosebnih podatkov, da bi podjetja, vključno z malimi in srednjimi podjetji, bolje razumela medsebojni vpliv med to uredbo in Uredbo (EU) 2016/679 ter zagotovila skladnost z obema uredbama.
- (38) Ta uredba spoštuje temeljne pravice in upošteva načela, ki jih priznava zlasti Listina Evropske unije o temeljnih pravicah, ter bi jo bilo treba razlagati in uporabljati v skladu z navedenimi pravicami in načeli, vključno s pravicami do varstva osebnih podatkov, do svobodnega izražanja in obveščanja in do svobode gospodarske pobude.
- (39) Ker cilja te uredbe, in sicer zagotoviti prosti pretok podatkov, ki niso osebni podatki, v Uniji, ni mogoče zadovoljivo doseči na ravni držav članic, temveč se zaradi njegovega obsega in učinkov lažje doseže na ravni Unije, lahko Unija sprejme ukrepe v skladu z načelom subsidiarnosti iz člena 5 PEU. V skladu z načelom sorazmernosti iz navedenega člena ta uredba ne presega tistega, kar je potrebno za doseganje navedenega cilja –

⁽¹⁾ Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (UL L 194, 19.7.2016, str. 1).

SPREJELA NASLEDNJO UREDBO:

Člen 1

Predmet urejanja

Namen te uredbe je zagotoviti prosti pretok podatkov, ki niso osebni podatki, v Uniji z določitvijo pravil z zvezi z zahtevami glede lokalizacije podatkov, razpoložljivostjo podatkov za pristojne organe in prenosom podatkov za poklicne uporabnike.

Člen 2

Področje uporabe

1. Ta uredba se uporablja za obdelavo elektronskih podatkov, ki niso osebni podatki, v Uniji, ki:
 - (a) se opravlja kot storitev za uporabnike, ki prebivajo ali imajo sedež v Uniji, ne glede na to, ali ima ponudnik storitev sedež v Uniji ali ne, ali
 - (b) jo izvaja fizična ali pravna oseba, ki prebiva ali ima sedež v Uniji, za lastne potrebe.
2. V primeru podatkovnega niza, ki vsebuje osebne in neosebne podatke, se ta uredba uporablja za del podatkovnega niza, ki obsega neosebne podatke. Kadar so osebni in neosebni podatki v podatkovnem nizu neločljivo povezani, ta uredba ne posega v uporabo Uredbe (EU) 2016/679.
3. Ta uredba se ne uporablja za dejavnosti, ki ne spadajo na področje uporabe prava Unije.

Ta uredba ne posega v zakone in druge predpise v zvezi z notranjo organizacijo držav članic, ki določajo prenos pristojnosti in pooblastil za obdelavo podatkov brez pogodbenih plačil zasebnih strank na javne organe in osebe javnega prava, kakor so opredeljene v točki (4) člena 2(1) Direktive 2014/24/EU, kot tudi ne v zakone in druge predpise držav članic, ki določajo izvajanje teh pooblastil in pristojnosti.

Člen 3

Opredelitev pojmov

V tej uredbi se uporabljajo naslednje opredelitve pojmov:

- (1) „podatki“ pomeni podatke, ki niso osebni podatki, kakor so opredeljeni v točki (1) člena 4 Uredbe (EU) 2016/679;
- (2) „obdelava“ pomeni vsako dejanje ali niz dejanj, ki se izvaja v zvezi s podatki ali nizi podatkov v elektronski obliki z avtomatiziranimi sredstvi ali brez njih, kot je zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje;
- (3) „osnutek akta“ pomeni besedilo, oblikovano z namenom, da bo sprejeto kot zakon ali drug splošni predpis, pri čemer je besedilo v fazi priprave, v kateri se lahko še vedno bistveno spremeni;
- (4) „ponudnik storitev“ pomeni fizično ali pravno osebo, ki opravlja storitve obdelave podatkov;
- (5) „zahteva glede lokalizacije podatkov“ pomeni kakršno koli obveznost, prepoved, pogoj, omejitev ali drugo zahtevo, ki je določena v zakonih ali drugih predpisih države članice ali izhaja iz splošne in dosledne administrativne prakse v državi članici in osebah javnega prava, vključno s tistimi, povezanimi z javnim naročanjem, brez poseganja v Direktivo 2014/24/EU, in ki določa, da mora obdelava podatkov potekati na ozemlju določene države članice ali omejuje obdelavo podatkov v drugi državi članici;
- (6) „pristojni organ“ pomeni organ države članice ali kateri koli drug subjekt, pooblaščen v skladu z nacionalnim pravom za opravljanje javne funkcije ali izvajanje javne oblasti, ki je pooblaščen, da za opravljanje svojih uradnih dolžnosti pridobi dostop do podatkov, ki jih obdeluje fizična ali pravna oseba, kot je določeno s pravom Unije ali nacionalnim pravom;
- (7) „uporabnik“ pomeni fizično ali pravno osebo, vključno z javnim organom ali osebo javnega prava, ki uporablja ali naroči storitev obdelave podatkov;
- (8) „poklicni uporabnik“ pomeni fizično ali pravno osebo, vključno z javnim organom ali osebo javnega prava, ki uporablja ali naroči storitev obdelave podatkov za namene v zvezi s svojo trgovsko, poslovno, obrtno ali poklicno dejavnostjo oziroma izpolnjevanjem nalog.

Člen 4

Prosti pretok podatkov v Uniji

1. Zahteve glede lokalizacije podatkov so prepovedane, razen če so utemeljene na podlagi javne varnosti ob upoštevanju načela sorazmernosti.

Prvi pododstavek tega odstavka ne posega v odstavek 3 in v zahteve glede lokalizacije podatkov, ki temeljijo na obstoječem pravu Unije.

2. Države članice v skladu s postopki iz členov 5, 6 in 7 Direktive (EU) 2015/1535 Komisijo nemudoma obvestijo o vsakem osnutku akta, s katerim se uvaja nova zahteva glede lokalizacije podatkov ali spreminja obstoječa zahteva glede lokalizacije podatkov.

3. Države članice do 30. maja 2021 zagotovijo, da se vse obstoječe zahteve glede lokalizacije podatkov, ki so določene z zakonom ali drugim splošnim predpisom in ki niso v skladu z odstavkom 1 tega člena, razveljavijo.

Če država članica do 30. maja 2021 meni, da je obstoječi ukrep, ki vsebuje zahtevo glede lokalizacije podatkov, v skladu z odstavkom 1 tega člena, in lahko zato ostane v veljavi, o tem ukrepu, skupaj z utemeljitvijo ohranitve njene veljavnosti, obvesti Komisijo. Brez poseganja v člen 258 PDEU Komisija v šestih mesecih od datuma prejema takega sporočila preveri skladnost navedenega ukrepa z odstavkom 1 tega člena in, kadar je ustrezno, zadevni državi članici poda pripombe, po potrebi skupaj s priporočilom, naj ukrep spremeni ali razveljavi.

4. Države članice zagotovijo javno dostopnost podrobnosti o vseh zahtevah glede lokalizacije podatkov, določenih v zakonu ali drugem splošnem predpisu, ki se uporabljajo na njihovem ozemlju, prek nacionalne enotne spletne informacijske točke in te informacije posodablja ali posodobljene informacije o vseh zahtevah glede lokalizacije podatkov posredujejo centralni informacijski točki, vzpostavljeni v skladu z drugim aktom Unije.

5. Države članice obvestijo Komisijo o naslovu svoje enotne informacijske točke iz odstavka 4. Komisija objavi povezave do teh točk na svojem spletišču, skupaj z redno posodobljenim zbirnim seznamom vseh zahtev glede lokalizacije podatkov iz odstavka 4, vključno s povzetimi informacijami o teh zahtevah.

Člen 5

Razpoložljivost podatkov za pristojne organe

1. Ta uredba ne vpliva na pooblastila pristojnih organov, da za opravljanje svojih uradnih dolžnosti v skladu s pravom Unije ali nacionalnim pravom zahtevajo ali pridobijo dostop do podatkov. Dostop pristojnih organov do podatkov se ne sme zavrniti na podlagi dejstva, da se podatki obdelujejo v drugi državi članici.

2. Kadar pristojni organ potem, ko je zahteval dostop do podatkov uporabnika, dostopa ne pridobi in če ne obstajajo posebni mehanizmi sodelovanja v okviru prava Unije ali mednarodnih sporazumov za izmenjavo podatkov med pristojnimi organi različnih držav članic, lahko ta pristojni organ v skladu s postopkom iz člena 7 zaprosi za pomoč pristojni organ v drugi državi članici.

3. Kadar prošnja za pomoč vključuje, da zaproseni organ pridobi dostop do prostorov fizične ali pravne osebe, vključno z vso opremo in sredstvi za obdelavo podatkov, mora biti takšen dostop v skladu s pravom Unije ali nacionalnim postopkovnim pravom.

4. Države članice lahko v skladu s pravom Unije in nacionalnim pravom določijo učinkovite, sorazmerne in odvračilne kazni za neupoštevanje obveznosti zagotovitve podatkov.

V primeru, ko uporabnik zlorabi pravice, lahko država članica, kadar je to upravičeno zaradi nujnosti dostopa do podatkov, in ob upoštevanju interesov zadevnih strani, določi strogo sorazmerne začasne ukrepe v zvezi s tem uporabnikom. Če začasni ukrep določa relokalizacijo podatkov za obdobje, ki je daljše od 180 dni, mora biti Komisija o tem obveščena v tem 180-dnevnem obdobju po relokalizaciji. Komisija v najkrajšem možnem času preuči ukrep in njegovo združljivost s pravom Unije ter, kadar je to ustrezno, sprejme potrebne ukrepe. Komisija izmenjuje informacije z enotnimi kontaktnimi točkami držav članic iz člena 7 o izkušnjah, pridobljenih v zvezi s tem.

Člen 6

Prenos podatkov

1. Komisija spodbuja in olajšuje pripravo samoregulativnih kodeksov ravnanja na ravni Unije (v nadaljnjem besedilu: kodeksi ravnanja), da se prispeva h konkurenčnemu podatkovnemu gospodarstvu, ki temeljijo na načelih preglednosti in interoperabilnosti in ustrezno upoštevajo odprte standarde, ki med drugim zajemajo naslednje vidike:
 - (a) najboljše prakse za lažjo zamenjavo ponudnika storitev in lažji prenos podatkov v strukturirani, splošno uporabljani in strojno berljivi obliki, vključno s formati odprtih standardov, kadar je to potrebno ali če to zahteva ponudnik storitev, ki sprejema podatke;
 - (b) zahteve za minimalne informacije, da se profesionalnim uporabnikom pred sklenitvijo pogodbe za obdelavo podatkov zagotovijo dovolj podrobne, jasne in pregledne informacije v zvezi s postopki, tehničnimi zahtevami, roki in stroški, ki se uporabljajo v primeru, da poklicni uporabnik želi zamenjati ponudnika storitev ali prenesti podatke nazaj v lastne informacijske sisteme;
 - (c) pristope k certifikacijskim shemam, ki olajšujejo primerjavo proizvodov in storitev obdelave podatkov za poklicne uporabnike, ob upoštevanju ustaljenih nacionalnih ali mednarodnih norm, ki olajšujejo primerljivost teh proizvodov in storitev. Ti pristopi lahko med drugim vključujejo upravljanje kakovosti, upravljanje informacijske varnosti, upravljanje neprekinjenosti poslovanja in okoljsko upravljanje;
 - (d) komunikacijske načrte, ki temeljijo na multidisciplinarnem pristopu, za ozaveščanje o kodeksih ravnanja med ustreznimi deležniki.
2. Komisija zagotovi, da se kodeksi ravnanja razvijejo v tesnem sodelovanju z vsemi ustreznimi deležniki, vključno z združenji malih in srednjih ter zagonskih podjetij, uporabniki in ponudniki storitev v oblaku.
3. Komisija spodbuja ponudnike storitev, naj pripravo kodeksov ravnanja zaključijo do 29. novembra 2019 in naj jih dejansko začnejo izvajati do 29. maja 2020.

Člen 7

Postopek za sodelovanje med organi

1. Vsaka država članica imenuje enotno kontaktno točko, ki je v zvezi z uporabo te uredbe v stiku z enotnimi kontaktnimi točkami drugih držav članic in Komisijo. Države članice uradno obvestijo Komisijo o imenovanih enotnih kontaktnih točkah in njihovih morebitnih poznejših spremembah.
2. Kadar pristojni organ v eni državi članici zaprosi drugo državo članico za pomoč v skladu s členom 5(2) za pridobitev dostopa do podatkov, na enotno kontaktno točko, ki jo imenuje zaprosena država članica, naslovi ustrezno utemeljeno prošnjo. Prošnja vključuje pisno pojasnilo razlogov in pravno podlago za pridobitev dostopa do podatkov.
3. Enotna kontaktna točka določi ustrezen pristojni organ svoje države članice in prošnjo, prejeto v skladu z odstavkom 2, posreduje temu pristojnemu organu.
4. Na ta način zaproseni ustrezeni pristojni organ brez nepotrebnega odlašanja in v časovnem okviru, ki je sorazmeren z nujnostjo prošnje, odgovori tako, da pristojnemu organu prosilcu sporoči zahtevane podatke ali ga obvesti o svojem stališču, da prošnja za pomoč ne izpolnjuje pogojev v skladu s to uredbo.
5. Vse informacije, izmenjane v okviru pomoči, ki se zaprosi in zagotovi v skladu s členom 5(2), se uporabljajo samo v zvezi z zadevo prošnje za pomoč.
6. Enotne kontaktne točke uporabnikom zagotavljajo splošne informacije o tej uredbi, vključno z informacijami o kodeksih ravnanja.

Člen 8

Ocena in smernice

1. Komisija najpozneje 29. novembra 2022 predloži poročilo Evropskemu parlamentu, Svetu in Evropskemu ekonomsko-socialnemu odboru, v katerem oceni izvajanje te uredbe, zlasti glede:
 - (a) uporabe te uredbe in predvsem njene uporabe pri podatkovnih nizih, ki vsebujejo osebne in neosebne podatke, ob upoštevanju razvoja trga in tehnološkega razvoja, ki bi lahko razširil možnosti za deanonimizacijo podatkov;

- (b) izvajanja člena 4(1) s strani držav članic, zlasti izjeme glede javne varnosti, ter
 - (c) priprave in učinkovitega izvajanja kodeksov ravnanja ter učinkovitega zagotavljanja informacij s strani ponudnikov storitev.
2. Države članice zagotovijo Komisiji vse potrebne informacije za pripravo poročila iz odstavka 1.
3. Komisija do 29. maja 2019 objavi informativne smernice o medsebojnem vplivu med to uredbo in Uredbo (EU) 2016/679, zlasti kar zadeva podatkovne nize, ki vsebujejo osebne in neosebne podatke.

Člen 9

Končne določbe

Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Ta uredba se začne uporabljati šest mesecev po njeni objavi.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Strasbourgu, 14. novembra 2018

Za Evropski parlament

Predsednik

A. TAJANI

Za Svet

Predsednica

K. EDTSTADLER
